ROBERT T. HASLAM (Bar No. 071134)
ROBERT D. FRAM (Bar No. 126750)
SARAH E. MITCHELL (Bar No. 187053)
HELLER EHRMAN WHITE & McAULIFFE
525 University Avenue
Palo Alto, California 94301-1900
Telephone (415) 324-7000

268

CSW

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ROGER SCHLAFLY,

Plaintiff,

v.

PUBLIC KEY PARTNERS, a partnership, and RSA DATA SECURITY, INC., a California corporation,

Defendants.

Case No. CV-94-20512-SW (EAI)

DECLARATION OF SARAH E. MITCHELL IN SUPPORT OF RSA DATA SECURITY, INC.'S MOTION FOR SUMMARY JUDGMENT ON PLAINTIFF'S NON-INFRINGEMENT CLAIM

I, Sarah E. Mitchell, declare:

1. I am an attorney at HELLER EHRMAN WHITE & McAULIFFE and counsel of record for Defendant RSA DATA SECURITY, INC. ("RSA") herein and I have personal knowledge concerning the facts set forth below. If called upon to testify, I would and could testify competently thereto.

2. The exhibits attached hereto are excerpts from the prosecution history of United States Patent No. 4,405,829 [the RSA Patent].

3. Attached hereto as Exhibit A is a true and correct copy of an Office Action of the United States Patent and Trademark Office dated December 15, 1978.

4. Attached hereto as Exhibit B is a true and correct copy of an amendment that was filed with the United States Patent and Trademark Office dated May 15, 1979.

5. Attached hereto as Exhibit C is a true and correct copy of the United States Patent and Trademark Office Examiner's Interview Summary Record dated August 6, 1979.

6. Attached hereto as Exhibit D is a true and correct copy of an Office Action of the United States Patent and Trademark Office dated August 6, 1979.

I declare under penalty of perjury, under the laws of the United States of America, that the foregoing is true and correct.

Executed on July 23, 1997, at Palo Alto, California.

Sarah E Mitchell

Sarah E. Mitchell

A

PAPER NO. 5

[illegible]
[illegible]
[illegible] 11/77

U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

MAILED

MAILED
DEC 15 1978

[Ronald L. Rivest, et. al.
[illegible] 12/14/77 860,586]

Arthur A. Smith, Jr.
Mass. Institute of Technology
Room E19-722
Cambridge, Mass. 02139

THIS IS A COMMUNICATION FROM THE EXAMINER IN CHARGE OF YOUR APPLICATION.

COMMISSIONER OF PATENTS AND TRADEMARKS

☑ This application has been examined.

□ Responsive to communication filed on ________.

□ This action is made final.

A SHORTENED STATUTORY PERIOD FOR RESPONSE TO THIS ACTION IS SET TO EXPIRE 3 MONTH(S) 0 DAYS FROM THE DATE OF THIS LETTER.

FAILURE TO RESPOND WITHIN THE PERIOD FOR RESPONSE WILL CAUSE THE APPLICATION TO BECOME ABANDONED. 35 U.S.C. 133

PART I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. ☑ Notice of References Cited, Form PTO-892.
2. □ Notice of Informal Patent Drawing, PTO-948.
3. □ Notice of Informal Patent Application, Form PTO-152
4. □

PART II SUMMARY OF ACTION

1. ☑ Claims 1-33 are pending in the application.

   Of the above, claims ________ are withdrawn from consideration.

2. □ Claims ________ have been cancelled.

3. □ Claims ________ are allowed.

4. ☑ Claims 1-33 are rejected.

5. □ Claims ________ are objected to.

6. □ Claims ________ are subject to restriction or election requirement.

7. □ The formal drawings filed on ________ are acceptable.

8. □ The drawing correction request filed on ________ has been □ approved. □ disapproved.

9. □ Acknowledgement is made of the claim for priority under 35 U.S.C. 119. The certified copy has □ been received. □ not been received. □ been filed in parent application; serial no. ________ filed on ________.

10. □ Since this application appears to be in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under Ex parte Quayle, 1935 C.D. 11, 453 OG 213.

11. □ Other

FORM PTO 46-59
(5-77) Formerly PTO-1142

U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

PART III

SERIAL NUMBER 86-C, 586

GROUP ART UNIT 222

NOTIFICATION OF REJECTION(S) AND/OR OBJECTION(S) (35 USC 132)

•	CLAIMS 11	REASONS FOR REJECTION 12	REFERENCES * 13	INFORMATION IDENTIFICATION AND COMMENTS 14
1	1-33	35USC101	R	TAKEN IN LIGHT OF THE PRIOR ART PUBLIC KEY TEACHINGS OF (R), THE PRESENT INVENTION AS CLAIMED LIES IN A PARTICULAR ALGORITHM WHICH IS EMPLOYED TO IMPLEMENT THE PUBLIC KEY CRYPTOGRAPHY SCHEME. WHERE THE INVENTION LIES IN THE ALGORITHM (cont below, line 5)
2				
3				
4				

5 cont AS THE CLAIMS DEFINE, THE SAME DOES NOT FALL WITHIN THE STATUTORY CATEGORIES OF INVENTION DEFINED BY 35USC101, AS IN PARKER V FLOOK, 198USPQ193, AND GOTTSCHALK V BENSON, 175USPQ673.

6 APPLICANT'S CITATIONS OF PRIOR ART HAVE BEEN CONSIDERED AND THOSE FELT TO BE PERTINENT HAVE BEEN MADE OF RECORD.

* Capital letters representing references are identified on accompanying Form PTO 46-42. (Formerly PTO-892)
The symbol "v" between letters represents - in view of -.
The symbol "+" or "&" between letters represents - and -.
A slash "/" between letters represents the alternative - or -.

NOTE- Sections 100, 101, 102, 103, and 112 of the Patent Statute (Title 35 of the United States Code) are reproduced on the back of this sheet.

EXAMINER

TEL. NO. (703) -557 -2897

Howard A. Birmiel

HOWARD A. BIRMIEL
EXAMINER
GROUP ART UNIT 222

TO SEPARATE, HOLD TOP AND BOTTOM EDGES. SNAP—APART AND DISCARD CARBON

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

NOTICE OF REFERENCES CITED

SERIAL NO.	GROUP ART UNIT	ATTACHMENT TO PAPER NUMBER
860,586	222	5

APPLICANT(S): RIVEST ET AL

U.S. PATENT DOCUMENTS

	DOCUMENT NO.	DATE	NAME	CLASS	SUB-CLASS	FILING DATE IF APPROPRIATE
A	3657476	4-72	Aiken	178	22	
B						
C						
D						
E						
F						
G						
H						
I						
J						
K						

FOREIGN PATENT DOCUMENTS

	DOCUMENT NO.	DATE	COUNTRY	NAME	CLASS	SUB-CLASS	PERTINENT SHTS. DWG.	PERTINENT PP. SPEC.
L								
M								
N								
O								
P								
Q								

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

✓ R "New Directions In Cryptography", Diffie et al, IEEE Transactions on Information Theory, Vol IT-22, No. 6, Nov. 1976, p644-654, copy in 178/22

✓ S "Theory of Numbers", Stewart, MacMillan Co, 1952, p133-135

✓ T Diffie et al, "Multi-User Cryptographic Techniques", AFIPS-Conference Proceedings, Vol. 45, p109-112, June 8, 1976, c/178/22

U

EXAMINER	DATE
Howard A. Birmiel	12/3/78

* A copy of this reference is not being furnished with this office action.
(See Manual of Patent Examining Procedure, section 707.05 (a).)

B

80cc 107 ic 22

9

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

B + [illegible]
L.W[illegible]
5/30/79

In the matter of the application of :
:
Ronald L. Rivest, Adi Shamir and :
Leonard M. Adleman :
: Examiner: H.A. Birmiel
Serial No: 860,586 ✓ :
:
Filed: December 14, 1977 : Group Art Unit: 222
:
For: CRYPTOGRAPHIC COMMUNICATIONS :
SYSTEM AND METHOD :

AMENDMENT A

Hon. Commissioner of Patents
Washington, D.C. 20231

Dear Sir:

This paper is responsive to the Office Action of December 15, 1978. Please amend the above-referenced application as follows:

IN THE CLAIMS:

Add the following claims:

34. A system according to claims 1 or 2 or 3 or 4 or 5 or 6 or 7 or 8 or 9 or 10 or 11 or 12 or 13 or 14 or 15 or 16 or 17 or 28 or 29 or 30 wherein at least one of said transforming means comprises:

a first register means for receiving and storing a first digital signal representative of said word-to-be-transformed,

a second register means for receiving and storing a second digital signal representative of the exponent of the equivalence relation defining said transformation,

a third register means for receiving and storing a third digital signal representative of the modulus of the equivalency relation defining said transformation, and

ck 7600

an exponentiation by repeated squaring and multiplication network coupled to said first, second and third register means, said network including:

A. an output register means for receiving and storing a first multiplier signal and for applying said first multiplier signal to a first multiplier input line,

B. selector means for successively selecting each of the bits of said second digital signal as a multiplier selector signal,

C. means operative for each of said multiplier selector signals for selecting as a second multiplier signal either the contents of said output register means or the contents of said first register means, and for said second applying multiplier signal to a a second ultiplier input line, said selection being dependent on the binary value of the successive bits of said second digital signal, and

D. modulo multiplier means operative in step with said selector means and responsive to said first and second multiplier signals on said first and second multiplier input lines for successively generating first multiplier signals and for transferring said first multiplier signals to said output register means, said first multiplier signal initially being representative of binary 1, and thereafter being representative of the modulo product of said first and second multiplier signals, where the modulus of said modulo product corresponds to said third digital signal.

35. A method according to claims 18 or 19 or 20 or 21 or 22 or 23 or 24 or 25 or 26 or 27 or 31 or 32 or 33 wherein at least one of said transforming means comprises the steps of:

receiving and storing a first digital signal in a first register, said first digital signal being representative of said word-to-be-transformed,

receiving and storing a second digital signal in a second register, said second digital signal being representative of the exponent of the equivalence relation defining said transformation,

receiving and storing a third digital signal in a third register, said third digital signal being representative of the modulus of the equivalency relation defining said transformation, and

exponentiating said first digital signal by repeated squaring and multiplication using said second and third digital signals, said exponentiating step including the substeps of:

A. receiving and storing a first multiplier signal in an output register, and applying said first multiplier signal to a first multiplier input line,

B. successively selecting each of the bits of said second digital signal as a multiplier selector, and

C. for each of said multiplier selectors, selecting as a second multiplier signal either the contents of said output register or the contents of said first register, and for applying said second multiplier signal to a second multiplier output line, said selection being dependent on the binary value of the successive bits of said second digital signal,

D. for each of said multiplier selectors, generating said first multiplier signal in a modulo multiplier in response to the first and second multiplier signals on said first and second multinlier inout lines, and for transferring said generated first multiplier signal to said output register, said first multiplier signal initially beinq representative of binary 1 and thereafter beinq representative of the modulo product of said first and second multipliers, where the modulus of said modulo product corresponds to said third digital signal.

REMARKS:

The applicants' attorney gratefully acknowledges the Examiner's efforts extended at the interview of March 2, 1979.

Initially, it is noted that new claims 34 and 35 have been added. These claims are directed to cover applicants' invention in the form shown in Fig. 3. As agreed to by the Examiner at the interview, Fig. 3 clearly has sufficient hardware to support allowable claims. Accordingly, it is submitted that claims 34 and 35 are at least allowable combined with the claims from which they depend.

In the Office Action, all of claims 1-33 were rejected under 35 U.S.C. 101 as being directed to non-statutory subject matter. Issue is taken with that position.

In the rejection, the Examiner states that "the present invention as claimed lies in a particular algorithm which is employed to implement the public key cryptography scheme of Diffie and Hellman (reference R). However, there are no mathematical algorithms in the applicants' claims.

The expressions in the applicants' claims which include the symbol "≡" denote the well-known equivalence relation: congruence modulo m, for integers. The symbol "≡" merely is a shorthand notation (invented by Gauss in 1801) for expressing this equivalence relation to relate sets of numbers shown on either side of that symbol, in effect establishing a set of conditions between the related integers, or signals representative thereof. In Van Norstrand's Scientific Encyclopedia (Van Norstrand Reinhold Company, 1976, page 64), this equivalence relation is defined as follows:

> Two elements a, b of a ring are
> congruent modulo m, written
> a ≡ b (mod m), if there exist
> elements p, q, r in the ring
> such that a = mp+r, b = mq+r .

Also see Stewart, B.M., Theory of Numbers, MacMillan Company, New York, 1952, pages 111, 112 (copy enclosed). Thus, the symbol "≡" is a symbol for "congruence", not arithmetic or mathematical "equality", and the fact that the equivalence relation of the form

$$A \equiv B^{C} (\mathrm{mod}\ n)$$

is in the claims does not introduce a mathematical formula or algorithm to the claims but rather describes a relationship between two signals, e.g. the message and ciphertext. More particularly, in the applicants' claims, the message M and the ciphertext C are related by the transformation performed by the encoding means and the ciphertext C is related to the receive message word M' by the transformation performed by the decoding emans. The claims include a description of these relationships, but do not specify any algorithms for effecting the transformations.

It should be noted that there may be many algorithms

91

which may be used to obtain the various terms for the relation. For example, the "exponentiation by repeated squaring and multiplication" approach shown by applicants' in the preferred embodiment is but one way of finding terms satisfying the relation. However, applicants do not claim any particular algorithms. In fact, any algorithms which may be used in practicing applicants' invention may readily be used in other applications without being covered by the applicants' claims.

Thus, the applicants' claimed invention does not "lie in an algorithm" which is employed to implement the Diffie and Hellman scheme, as characterized by the Examiner, but rather resides in a step of or means for transforming an input signal to an output signal in a communications system so that the output signal is related to the input signal by the specified equivalency relation, regardless of the particular technique or algorithm employed in performing that transformation.

Moreover, it appears that the §101 rejection would not have even come into play in this case if the expressions of the equivalency relation were not present. This may be seen if it is assumed for the moment that the encoding and decoding (i.e. transforming) means of claim 1 were simple transformation means, for example, digital complimenting or inverter circuits. Then, the claim could have the form:

> A cryptographic communications system comprising:
>
> A. a communications channel
>
> B. an encoding means coupled to said channel including means for digitally <u>inverting</u> a transmit message word M to form a ciphertext word C and for transmitting C on said channel
>
> C. a decoding means coupled to said channel and adapted for receiving C from said

> channel and for inverting C to form a receive message word M'.

This hypothetically claimed system has three basic elements: a communication channel and two inverters coupled thereto. The inverters perform a "mathematical transformation" on the signal applied to them. There is no algorithm specified for performing the inversion, but only a requirement that the ciphertext be related to the message by the complementing relation.

Assuming that digital complementing was a suitable transformation for the invention, and that the claimed structure satisfied 102 and 103, then there would be no question that the claims would be allowable. Section 101 would quite properly not come into play since there are merely three interconnected hardware elements. In the present case, the encoding and decoding means are merely somewhat more complex building blocks than inverter circuits, where each block performs a transformation on input signals applied to the block. As in the hypothetical claim, there is no particular formula or algorithm specified for the transformation in the applicants' claims--only that the resultant signal be related to the input signal by the stated equivalency relation.

The applicants merely use such a building block. While at the present time there may not be any single chip implementations of that building block available, the block may be readily built by those skilled in the art, for example by merely implementing the circuit shown in Fig. 3. The applicants by their claims certainly do not preempt the transformation performed by the building block. For these reasons, the Examiner's position that the claimed invention "lies in a particular algorithm" is incorrect. Accordingly, the rejection should be reconsidered and withdrawn.

It is also noted that the rejection was applied against claims 1-17 and 28-30 which are system claims, as well as claims 18-27 and 31-33 which are method claims.

Regarding the method claims 18-27 and 31-33, the Examiner stated that the "invention as claimed lies in a particular algorithm . . .", citing Parker v. Flook, 198 U.S.P.Q. 193 and Gottschalk v. Benson, 175 U.S.P.Q. 673. The Examiner appears to use the term "algorithm" synonymously with the term "mathematical formula" found, for example, in the Benson case. The present invention, as claimed, does not fall within the proscribed subject matter of the Benson case, because it does not seek to patent a mathematical formula, and hence does not seek to patent an "algorithm" within the definition of mathematical formula set forth by Benson and Flook. As noted above, the claims 18-27 and 31-33 do not claim mathematical formulae but merely include expressions of an equivalence relation to pose conditions (expressed in Gauss' shorthand notation) on the claimed transformations.

The Court in Flook noted that "the only novel feature of the method is a mathematical formula", 198 U.S.P.Q. at 195. The Court goes on to state in footnote 1 on page 195 that "we use the word "algorithm" in this case as we did in Gottschalk v. Benson, ..., to mean "a procedure for solving a given type of mathematical problem...". The subject matter claimed in the present case is neither a procedure for solving a mathematical problem, nor a hitherto unknown mathematical formula or a sequence of such mathematical formulae, but is instead the application of one or more process steps to establish cryptographic communications and to provide authentication of digital messages.

While some of these steps may be, and in fact are, expressed in part with an equivalence relation (i.e. using Gauss' shorthand notation), that fact does not implicate that those steps are claims to a mathematical formula or algorithm. In the present case, the applicants' claimed steps do not claim a mathematical formula or algorithm. This may be better seen if, for example, lines 13 and 14 of claim 18 were changed from "whereby $C \equiv M^e$ (mod n)" to an equivalent form which reads "by selecting C so that the difference between C and the eth power of M is an integer multiple of n." Clearly, there is no "algorithm" in this form of the claim. It does not matter how C is selected. For example, C may be selected by "trial-and-error", or alternatively by "exponentiation-by-repeated-squaring" (as in the applicants' preferred embodiment) or some other method. The exponentiation-by-repeated-squaring approach is of course considerably more efficient in terms of hardware implementation. But is is important to note that <u>the claims are independent of any particular method (or algorithm)</u> for finding the terms to satisfy the relation. All that matters is that these terms be found -- by any method or algorithm. This same reasoning is applicable to all of claims 1-33. Thus, the claimed invention is not a proscribed "algorithm" within 35 U.S.C. 101.

The CCPA cases which have evolved in the face of <u>Benson</u> and <u>Flook</u> (and which have not been reversed), cases such as <u>In re Chatfield</u>, 191 USPQ 730 (CCPA 1976), <u>In re Freeman</u>, 197 USPQ 464 (CCPA 1978), and <u>In re Johnson</u>, <u>et al</u>., 200 USPQ 199 (CCPA 1978), clearly support the proposition that the invention claimed herein is patentable under 35 U.S.C. 101. The Johnson decision (which was handed down after the Office Action herein) is particularly informative since it follows (in time and substance) the <u>Flook</u>

decision. In Johnson, the CCPA states:

> "[I]t is clear after Flook that the board's conclusion that patent protection is proscribed for all inventions algorithmic in character is overbroad and erroneous."
> (200 USPQ at 205)

The CCPA in Johnson further went on to solidify the definition of an algorithm, citing Chatfield, wherein they stated:

> "The Supreme Court carefully supplied a definition of the particular algorithm before it, i.e., [a] procedure for solving a given type of mathematical problem.
>
> "The broader definition of algorithm is a step-by-step procedure for solving a problem or accomplishing some end.... It is axiomatic that inventive minds seek and develop solutions to problems and step-by-step solutions often attain the status of patentable invention. It would be unnecessarily detrimental to our patent system to deny inventors patent protection on the sole ground that their contribution could be broadly termed an 'algorithm'."
> (200 USPQ at 206-207)

The CCPA then went on to review the two step analytical approach taken in Freeman to determine whether or not the claims before it were patentable. The Court of Customs and Patent Appeals in Freeman dealt with method claims similar in form to the method claims rejected in the present case. The CCPA's analysis in that decision is directly applicable here. In Freeman, the Court set forth a two-step analysis for determination of whether a claim is directed to non-statutory subject matter as a whole, in light of Benson:

> "First, it must be determined whether the claim directly or

> indirectly recites an 'algorithm' in the Benson sense of that term,....
>
> "Second, the claim must be further analyzed to ascertain whether in its entirety it wholly preempts that algorithm." (197 USPQ at 471)

In Freeman, the Court noted that every process may be characterized as a "step-by-step procedure...for accomplishing some end" and that therefore, it would be "absurd" to interpret the Supreme Court's view as encompassing all such processes. Even if that "absurd" interpretation were taken, in the present case, as discussed above, the rejected claims are not "algorithmic", in spite of the fact that the claims include an equivalence relation. That equivalence relation only expresses conditions on a transformation. The conditions expressed by that equivalence relation may not be characterized as "a step-by-step procedure...for accomplishing some end". Thus, the present rejection should be reconsidered and withdrawn for the same reasons cited in Freeman.

Even assuming that according to the first step of Freeman analysis, the process steps herein "directly or indirectly recite process steps which are themselves calculations, formulae, or equations" (which in applicants' opinion they do not), it is clear that the applicants' claims in no way wholly preempt any such calculations, formulae or equations. This may be seen, for example, by the fact that a congruency equivalence relation is found in the cipher system disclosed by the Stewart reference (copy enclosed with the applicants' prior art statement), but Stewart's approach is clearly not within the scope of the applicants' claims. Thus, the second step of the Freeman analysis leads to the inevitable conclusion that the claims herein clearly fall squarely within the Johnson analysis

5

and the present claims should be allowed.

Furthermore, following the remainder of Johnson reasoning, the CCPA elaborates upon its two part Freeman analysis to determine whether the claims recite mathematical algorithms which are non-statutory. Under the continuing second step analysis of the CCPA's reasoning, one

> "must determine whether each claim
> as a whole, including all of its
> steps, merely recites a mathematical
> formula or a method of calculation.
> This analysis requires careful
> interpretation of each claim in the
> light of its supporting disclosure
> to determine whether or not it
> merely defines a method of solving
> a mathematical problem. If it does
> not, then it defines statutory subject
> matter, namely, a 'process'".
> (200 USPQ 208, 209)

The invention in claims 18-27 and 31-33 is not directed to the solution of a mathematical problem, but rather solves the problem of privately transmitting a message over a communications channel and the problem of authentication (i.e. by providing digital signatures) of messages. The claims include the step of transforming a first signal to a second signal so that the second signal is related to the first by a stated equivalence relation. The method for doing so does not claim mathematical formulae and does not seek patents on a mathematical formula. Accordingly, the invention claimed herein clearly falls under the CCPA and Supreme Court reasonings.

For these reasons, the rejection of claims 18-27 and 31-33 under 35 U.S.C. 101 should be reconsidered and withdrawn.

With particular regard to system claims 1-17, and 28-30, it is noted that the Benson and Flook cases cited by the Examiner addressed method claims only. The Supreme Court in

Benson stated "The question is whether the method described and claimed is a 'process' within the meaning of the Patent Act." 175 USPQ at 674 (emphasis added). Similarly, in Flook, the Supreme Court addressed the question of whether a novel formula "makes an otherwise conventional method eligible for patent protection" 198 USPQ at 196. Thus, in both of the cited cases, the Supreme Court addressed "processes" under 35 U.S.C. 101.

In contrast, the claims 1-17 and 28-30 are all directed to apparatus including means to perform specified functions. Moreover, the claims are clearly supported in the specification by a hardware implementation of the claimed subject matter. Accordingly, the rejection of system claims 1-17 and 28-30 is inappropriate and should be reconsidered and withdrawn.

Moreover, even if the Examiner treats these system claims in the same manner as the method claims 18-27 and 31-33, the rejection should be withdrawn for the reasons discussed above in particular reference to the method claims.

For these reasons, the rejection of claims 1-33 under 35 U.S.C. 101 is inappropriate and should be withdrawn. It is submitted that these claims, as well as new claims 34 and 35 are in condition for allowance and passage to issue is requested.

Respectfully submitted,

KENWAY & JENNEY

By ______________________
Mark G. Lappin
Reg. No. 26,618

60 State Street
Boston, MA 02109
Tel: (617)227-6300
May 15, 1979

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents and Trademarks, Washington, D. C. 20231.

on MAY 15 1979
(Date of Deposit)

MARK G LAPPIN
Name of applicant, assignee, or Registered Representative

____
Signature

MAY 15 1979
Date of Signature

C

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address : COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
860,586	12-14-77	Ronald L. Rivest, et al.	

Arthur A. Smith, Jr.
Mass. Institute of Technology
Room E19-722
Cambridge, Mass. 02139

EXAMINER	
H.A. Birmiel	
ART UNIT	PAPER NUMBER
222	10

DATE MAILED:

EXAMINER INTERVIEW SUMMARY RECORD

All participants (applicant, attorney, agent) representing applicant:

(1) MR. LAPPIN (3) ____________

(2) ____________ (4) ____________

AUG 6 1979
GROUP 220

Date of interview ____________

Type: ☑ Telephonic □ Personal (copy is given to applicant).

Exhibit shown or demonstration conducted: □ Yes □ No.

Agreement ☑ was reached with respect to some or all of the claims in question. □ was not reached.

Claims discussed: 1-33 34-35

Identification of prior art discussed: ____________

Description of the general nature of what was agreed to if an agreement was reached, or any other comments:

APPLICANTS' ATTORNEY AGREED TO AMEND THE CLAIMS TO REFLECT THAT THE MATHEMATICAL TRANSFORMATIONS WERE PERFORMED UPON "SIGNALS" TO BETTER DEFINE THE SAME IN LIGHT OF THE 35 USC 101 REJECTION WHICH IS WITHDRAWN.
CLAIMS 34-35 ARE TO BE AMENDED TO REMOVE MULTIPLE DEPENDENCY.

(A fuller necessary description and any available copy of amendments that the examiner agreed would render the claims allowable, or where no copy of the amendments is available, a summary thereof, is attached.)

Howard L. Birmiel
HOWARD L. BIRMIEL
EXAMINER

□ It is not necessary for applicant to supplement the information on this form or to submit a separate record of the substance of the interview.

APPLICANTS, ATTORNEYS AND AGENTS ARE REMINDED OF THEIR RESPONSIBILITY TO SUPPLEMENT THE RECORD WITH AN INDICATION OF THE SUBSTANCE OF THE INTERVIEW AS REQUIRED BY 37 CFR 1.133(b) AND SECTION 713.04 OF THE MANUAL OF PATENT EXAMINING PROCEDURE. (See reverse side for text of Section 713.04.)

PTOL-413 (rev. 9/78)

ORIGINAL FOR INSERTION IN RIGHT HAND FLAP OF FILE WRAPPER

4.

D

UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

SERIAL NUMBER	FILING DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NO.
860,586	12/14/77	R.L. Rivest, et al.	

Arthur A. Smith, Jr.
Mass. Institute of Technology
Room E19-722
Cambridge, Mass. 02139

EXAMINER	
HABirmiel	
ART UNIT	PAPER NUMBER
222	11

DATE MAILED:

AUG 6 1979

GROUP 220

This is a communication from the examiner in charge of your application.
COMMISSIONER OF PATENTS AND TRADEMARKS

□ This application has been examined. ☑ Responsive to communication filed on 5/17/79 □ This action is made final.

A shortened statutory period for response to this action is set to expire 2 month(s), 0 days from the date of this letter.
Failure to respond within the period for response will cause the application to become abandoned. 35 U.S.C. 133

Part I THE FOLLOWING ATTACHMENT(S) ARE PART OF THIS ACTION:

1. □ Notice of References Cited, Form PTO-892.
2. □ Notice of Informal Patent Drawing, PTO-948.
3. □ Notice of Informal Patent Application, Form PTO-152.
4. □ ______

Part II SUMMARY OF ACTION

1. ☑ Claims 1-35 are pending in the application.

   Of the above, claims 34, 35 are withdrawn from consideration.
2. □ Claims ______ have been cancelled.
3. ☑ Claims 1-33 are allowed.
4. □ Claims ______ are rejected.
5. ☑ Claims 34, 35 are objected to.
6. □ Claims ______ are subject to restriction or election requirement.
7. □ The formal drawings filed on ______ are acceptable.
8. □ The drawing correction request filed on ______ has been □ approved. □ disapproved.
9. □ Acknowledgment is made of the claim for priority under 35 U.S.C. 119. The certified copy has □ been received. □ not been received. □ been filed in parent application, serial no. ______ filed on ______.
10. ☑ Since this application appears to be in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under Ex parte Quayle, 1935 C.D. 11; 453 O.G. 213.
11. □ Other

FTOL-326 (rev. 10-78)

EXAMINER'S FIRST ACTION

Claims 34 and 35 are objected to as not complying with 37 CFR 1.75 as of the filing date of this case. Specifically, multiple dependent claim practice is not permitted for applications filed prior to January 24, 1978, and the claims should be either amended or cancelled.

Claims 1-33 are allowed subject to applicants' insertion of the word "signal" and the like as discussed in a telephone interview of July 30. 1979.

HOWARD A. BIRMIEL
EXAMINER
GROUP ART UNIT 222

HABirmiel:lkj
(703) 557-2897
08/01/79